Mark A. Kleiman (SBN 115919)
KLEIMAN / RAJARAM
2525 Main Street, Suite 204
Santa Monica, CA 90405
Telephone: (310) 392-5455
Facsimile: (310) 306-8491
Email: mkleiman@quitam.org

Ben Gharagozli (SBN 272302)
Law Offices of Ben Gharagozli
2525 Main Street, Suite 204
Santa Monica, CA 90405
Telephone: (661) 607-4665
Facsimile: (855) 628-5517
Email: ben.gharagozli@gmail.com

Attorneys for Plaintiff, OMAR ABDULAZIZ

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OMAR ABDULAZIZ, Plaintiff, v. TWITTER, Inc..; McKINSEY & Co.; and DOES 1-10; inclusive, Defendants.	Case No.: 3:19 CV-06694-LB **PLAINTIFF, OMAR ABDULAZIZ'S OPPOSITION TO DEFENDANT, TWITTER, INC.'S MOTION TO DISMISS THIRD AMENDED COMPLAINT [ECF No. 99]** **Date: February 11, 2021** **Time: 9:30 a.m.** **Dept.: Courtroom B-15th Floor** **Judge: Hon. Laurel Beeler** **Action Filed: October 18, 2019** **Trial Date: None Set**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

UNITED STATES CONSTITUTION

CALIFORNIA STATUTES

OTHER AUTHORITIES

STATEMENT OF ISSUES TO BE DECIDED

1. Has Plaintiff pled a sufficient causal nexus between Twitter's conduct and his injuries for Article III standing?
2. Has Plaintiff pled facts to demonstrate proximate causation at the pleading stage?
3. Are Plaintiff's claims timely?
4. Are Twitter's Terms of Service ("TOS") insufficient to bar Plaintiff's claims?
5. Has Plaintiff properly pled the negligent supervision and retention claim?

MEMORANDUM OF POINTS AND AUTHORITIES

I. SUCCINCT STATEMENT OF THE RELEVANT FACTS

A. Plaintiff Began to Suffer Harm in 2015 Because of a 2014-2015 Breach Due to Twitter's Shoddy Security, Not His Public Criticisms That Began in 2009.

Twitter blames Plaintiff's public criticisms (which began in 2009) for harm he suffered starting in 2015. Yet, Twitter despite $2.2 billion in revenue, failed to meet industry standard safeguards that would have stopped inappropriate access to Plaintiff's data by restricting access to private user data and having humans address the alarms going off upon inappropriate access. This security failure let two KSA spies (Ahmad Abouammo and Ali Alzabarah) to raid private Twitter user data to furnish to KSA in 2015. At the end of 2015, KSA escalated its persecution of Plaintiff to an unprecedented level. (¶¶ 11-12, 49-50, 61, 67, 115) [1]

Aware of the risk of employees giving private data to third parties ("inside jobs"), Twitter's "Playbook" required employees to not disclose user data without Twitter's written consent; avoid conflicts of interest; and notify HR of gifts received exceeding $100, and return them. Abouammo and Alzabarah openly broke these rules. (¶¶ 13, 14, 81)

Twitter use was central to the "Arab Spring" 2010-2012, a wave of protests against Arab autocrats. KSA then clamped down on activists and greatly increased surveillance of Twitter. The fifth most frequently visited site in Saudi Arabia, Twitter is effectively the only place where Saudis can freely express themselves (Plaintiff says "Twitter is our Parliament"). (¶¶ 15-19)

[1] Cites using the "paragraph" ¶ sign are to Dkt. 98, the TAC, unless otherwise specified. Dkt. Page cites refer to the page number printed by the ECF at the top of each page of the document.

When Twitter hired Abouammo and Alzabarah in 2013, it knew about a threat of insiders accessing private data for dictators. Since at least 2009, authoritarian regimes repeatedly targeted tech companies. The FBI frequently warned social media platforms, including Twitter, of the insider threat well before 2015. Twitter had repeatedly been hacked before KSA agents raided private user data at Twitter's headquarters. Twitter's Board was also previously warned that giving employees broad access to user accounts was dangerous. (¶¶ 20-27).

B. Twitter Failed to Implement Industry Standard Security Safeguards.

Twitter failed to implement industry standard safeguards that would have restricted employee access to private data and prevent the inside job it knew was coming. Its insufficient human security meant (1) they had not implemented industry standards to protecting user data from inappropriate employee access; and/or (2) the alerts that sounded upon improper access to private data went unheeded,[2] and/or (3) Twitter's "Playbook" went unenforced, leaving Plaintiff and thousands of others unprotected from inappropriate access. (¶¶ 33, 35, 84-85).

Starting in December 2014, Abouammo accessed private user data for KSA for five months. From May 2015 to December 2015, Alzabarah invaded nearly 6,000 Twitter users' private data for KSA. Twitter failed to meet established industry standards of protecting access to private data. (¶¶ 11, 45, 52, 54, 61-70, 75-79, 87, 94) Abouammo and Alzabarah, exposed to KSA Plaintiff's pseudonymous account, IP address, password, private direct messages and phone number. Plaintiff relied on Twitter's assurances of privacy to speak freely with dissidents and activists who faced danger were KSA to learn of their beliefs and activities. (¶¶ 87-89).

C. Twitter Ruined the FBI's Investigation and Failed to Fix its Security.[3]

In late 2015, the FBI told Twitter it had a KSA mole (Alzabarah) and that the sensitive investigation was at an early stage. The FBI explicitly asked Twitter to not tell Alzabarah what

---

[2] Twitter had no financial incentive to have sufficient security safeguards because apparently, its entire privacy policy was just a lie anyway. See Dkt. 83, p. 24:12-14.

[3] Twitter, in its Motion to Dismiss, does not deny disregarding FBI requests to not notify Alzabarah. However, in fn. 4, Twitter does claim, without explanation, that refusing to comply with FBI's instructions designed to safeguard an investigation does not constitute negligence.

was going on as it could hurt the investigation. Twitter told him anyway. Justice Department officials were furious with Twitter for ruining their case against Alzabarah, who remains out of American reach.[4] Despite having authority and ability to detain Alzabarah for officials to arrest him after he admitted to crimes, Twitter suspended him, reclaimed the company laptop, and escorted him out. He fled the US the next day and escaped justice. Abouammo continued to inappropriately access information inside Twitter until March 1, 2016. (¶¶ 79-80, 86, 97-99)

Twitter then told the FBI in December 2015 it was greatly restricting access to user information. Yet, as of at least Summer 2020, over 1,000 employees and contractors could still access and even change user data in violation of industry standards. There have been so many account-spying episodes that Twitter's has given up trying to track them. The FBI has opened an investigation into Twitter for national security concerns. Former Twitter employees and at least one ex-FBI investigator noted that Twitter's focus on revenue eclipses security. (¶¶ 51, 115-117)

Twitter, quick to warn its employee decided to not issue a press release, not notify the popular press[5] as it would do with other data breaches and not tweet about this incident. It waited at least nine days before sending any notice (which Plaintiff did not even receive). At the time the Saudi Royalty owned more Twitter stock than CEO, Jack Dorsey. (¶¶ 100, 104, 113).

D. Plaintiff's Harm Began Less Than a Month After Twitter Tipped Off Alzabarah.

Within 30 days after Twitter ruined the FBI's case, KSA's campaign to silence Plaintiff unprecedentedly intensified: KSA targeted his family, friends and Twitter correspondents. Before, the worst KSA did was stop his financial aid. The timing of arrests of five other Saudi critics using anonymous Twitter accounts links to the Twitter breach. (¶¶ 94-95;120-122)

Plaintiff began publicly criticizing KSA in 2009. Yet it was not until December of 2015, the year Twitter employees raided his private twitter data and gave it to KSA, that KSA escalated

---

[4] Bradley Hope & Justin Scheck, "A Saudi Prince's Attempt to Silence Critics on Twitter". https://www.wired.com/story/mohammed-bin-salman-twitter-investigation/ Last visited November 1, 2020.

[5] None of the articles Twitter cite in fn.5 of its prior Motion (Dkt 83) mention information from a Twitter press release. The sources appear to be users who (unlike Plaintiff) got the December 02015 notice.

its persecution of Plaintiff by targeting his family and friends.[6] An MBS agent approached Plaintiff in 2017 to pressure Plaintiff to return to Saudi Arabia. Although Plaintiff greatly restricted his social media presence from January 2018 to July 2018, KSA continued its escalation. In mid-May 2018, two KSA agents told Plaintiff that MBS was upset with Plaintiff's political activities, attempted to lure Plaintiff to Saudi Arabia with promises of a bright future and tried to convince him to come with them to a Saudi embassy in Canada (the same tactics KSA used to murder Jamal Khashoggi a few months later). When that failed, KSA went further. Having purchased Pegasus spyware and training in 2017, KSA was finally able to deploy the malware in the spring of 2018 at the earliest. About a month after KSA's agents failed to silence Plaintiff and force him back to Saudi Arabia, Plaintiff's phone was one of the first KSA infected with Pegasus (giving KSA full access to Plaintiff's phone).[7] (¶¶ 8, 120-122, 130-136)

KSA got a vast amount of stolen private data from Abouammo and Alzabarah. Proper review would have taken KSA's intelligence agents months, if not years to perform to determine who to prioritize for an expensive hacking operation once technologies such as Pegasus finally became operational. Plaintiff was targeted because of the information Twitter employees had gleaned and furnished to KSA. Indeed, despite raiding thousands of Twitter Saudi dissident accounts, KSA targeted just a handful of dissidents for its Pegasus malware attack. Plaintiff is unaware of other Saudi dissident Twitter users KSA targeted with Pegasus. (¶¶ 123-125)

In late July 2018 and early August 2018 (approximately one month after the Pegasus hack), KSA forces raided Plaintiff's family home, conducted humiliating searches, imprisoned Plaintiff's brothers and dozens of his friends, political allies and people he had just messaged with. Plaintiff's brothers remain in prison without having been charged or tried. They have been tortured. KSA's security personnel even forced Plaintiff's younger brother to call him from

---

[6] Twitter Motion to Dismiss ignores the fact that KSA's persecution of Plaintiff was limited before the Twitter hack. (¶¶ 120-122)

[7] This was during the same period that KSA used Pegasus malware to target the phones of Dr. Aljabri and another prominent Saudi dissident (both of whom were living outside of Saudi Arabia). "Plaintiff was among the first Saudi dissidents KSA attacked with Pegasus." ¶ 135

prison to beg him to stop his political activities. Fearing for his safety, Plaintiff withdrew from his studies, fled his residence and lived out of hotels for months to avoid kidnapping and harm. (¶¶ 137-139, 141-142) Approximately two months after imprisoning Plaintiff's family and friends, KSA sent a hit team to travel to Canada to assassinate Dr. Aljabri and Plaintiff. (¶ 144)

II. ARGUMENT

A. Twitter's Article III Argument Distorts the TAC and the Court's Prior Order

1. The TAC Adequately Address the Court's August 12, 2020 Order.

Twitter argues the Court's August 12, 2020 order found the harms pled in the FAC did not plausibly establish that Twitter's alleged conduct caused these harms. (Dkt 99, 15:13-21). However, Twitter omits the two specific issues the Court's August 12th order had with the FAC, each of which the TAC has addressed. First, the Court noted that the FAC did "not explain how the compromise of the Twitter data caused the harm to his family and friends that happened shortly after Alzabarah fled to Saudi Arabia. Indeed, he is a political dissident with an active social-media presence who suffered persecution before the compromise of his Twitter data (shown by Canada's granting him political asylum in February 2014)." Second, the Court's order observed that the Pegasus malware was implanted three years after the compromise of his Twitter data and thus lacked temporal proximity. Further, the FAC did not disclose the time Plaintiff's family and friends in Saudi Arabia were targeted (Dkt. 76, 10-11).

As to the first issue, the TAC links Twitter's data breach and the harm Plaintiff suffered starting in December 2015. Plaintiff's asylum does not exonerate Twitter. Although Canada granted Plaintiff asylum in February 2014, the only persecution he suffered up to that point was KSA stopping Plaintiff's financial assistance. (¶¶ 120-122). His family had remained unharmed and free from KSA's persecution. (Id.) When Plaintiff applied for asylum in Canada in 2013, although he was afraid to return to Saudi Arabia, he was not worried that KSA would persecute his family and friends inside Saudi Arabia or send a hit team to kill him in Canada. (Id.)

As to the second issue, Plaintiff sufficiently pleads temporal proximity by alleging that within a month after Twitter tipped off Alzabarah and gave him reason and opportunity to flee on December 4, 2015, KSA began targeting Plaintiff's family and friends. This was unprecedented

and an escalation from KSA's prior cancellation of his financial assistance. From late December 2015 through 2018, KSA's campaign to silence Plaintiff gradually intensified. (¶¶ 94-95; 120-122, 130-141) This timeline unpacks events from 2009 to October 2018:

2009	Plaintiff moves to Canada and starts publicly criticizing KSA. (¶ 8)
December 2013	After KSA stopped its financial aid, Plaintiff applies for asylum. (¶ 120)
December 12, 2014-December 2, 2015	KSA spies working at Twitter access the private user data of thousands of Saudi dissidents including Plaintiff and furnish it to KSA. (See e.g. ¶¶ 46, 52-53, 61-63, 65-69, 76-78, 89, 91-94)
December 2, 2015	Despite explicit instructions from the FBI to not do so, Twitter confronts Alzabarah, one of the KSA spies working at Twitter, for raiding private user data for KSA . Alzabarah admits to accessing the information. Despite having the legal authority to detain Alzabarah so the FBI could arrest him, Twitter escorts him out of the building and suspends him. (¶ 98)
December 3, 2015	Alzabarah escapes the United States and resigns from Twitter. Justice Department officials were livid as Twitter had blown up their case by tipping off the man who they were hoping to arrest. (¶ 80)
December 2015-January 2016	KSA agents interrogate Plaintiff's father and brother in Saudi Arabia. KSA cancels Plaintiff's brother's financial assistance. (¶ 122)
March 2016-July 2016	KSA agents summon three of Plaintiff's friends and roommates in Canada for an interrogation in a Saudi government office. (¶ 122)
Between April and June 2017	An MBS agent in Canada tries to convince Plaintiff to return to Saudi Arabia at the same time MBS - was trying to lure Dr. Saad Aljabri (a former high-ranking KSA official who became an MBS opponent) back to Saudi Arabia to imprison, torture and/or murder him. (¶ 130)
January 2018 – July 2018	Plaintiff greatly restricts his social media presence but KSA continues escalating its persecution: Mid-May 2018, two KSA agents met with

	Plaintiff to demand that he stop his criticism and return to Saudi Arabia. Plaintiff refuses. They bring one of Plaintiff's brothers who is in their custody to the meeting to demonstrate their power over Plaintiff's family. (¶¶ 131-133, Dkt.38, ¶ 99)
Spring 2018	Pegasus malware becomes operational for the Saudi government. (¶ 135)
June 23, 2018	KSA infects Plaintiff's phone with Pegasus malware, getting full access to it. Plaintiff was one of a select few that KSA targeted with Pegasus despite raiding thousands of Twitter accounts. (¶ 135)
Late July 2018 to early August 2018	KSA 's security forces raid Plaintiff's family home in the middle of the night and conduct humiliating searches, imprison both of Plaintiff's brothers and dozens of his friends, political allies and correspondents. KSA personnel forced Plaintiff's brother to call Plaintiff from prison and beg him to stop his political activities. Plaintiff, fearing for his safety, withdraws from university and flees his residence, living in hotels for months to avoid kidnap and harm. (¶¶ 137-141)
October 2, 2018	KSA murders Jamal Khashoggi, Plaintiff's friend and ally. (¶ 144)
October 15, 2018	KSA's hit team ("Tiger Squad") travels to Canada with the intention of assassinating Dr. Saad Aljabri and Plaintiff. (¶ 146)

In an employment context, hostile action against an employee within 3-8 months of an employer learning the employee is a whistle blower "is easily within the time range that supports an inference of retaliation" and an eleven-month gap would also support such an inference. See Conszalter v. City of Salem, 320 F.3d 968, 977 (9th Cir. 2003); and Allen v. Iranon, 283 F.3d 1070, 1078 (9th Cir. 2002). Even so, Conszalter cautioned against mechanically applying a specified time period, as any number of reasons might slow a retaliator's timetable. Conszalter 320 F.3d at 977-978. Yet even if the Court were to start the clock from June/July 2015 as it did in the prior Order (Dkt. 76, p. 10) rather than December 2, 2015 when Twitter refused to listen to

the FBI and ruined the federal investigation by tipping off its employee Alzabarah, the harm Plaintiff suffered due to Twitter's negligent security standards started in December 2015 (five to six months after the Twitter raid). This temporal proximity supports an inference of causation.

2. The TAC Satisfies Article III's "Fairly Traceable Standard", Which Is a "Relaxed" Standard Exempt from *Iqbal* and *Twombly* Standards.

At the pleading stage, Plaintiff need not prove proximate causation. Plaintiff must merely show the injury is "fairly traceable to the challenged action". Daniel v. Nat'l Park Serv, 891 F.3d 762, 767 (9th Cir. 2017); see also Lexmark Int'l Inc. v. Static Control Components, Inc., 572 U.S. 118, n.6 (2014); Monsanto Co. v. Geertson Seed Farms, 561 U.S. 139, 149 (2010). This is a "relaxed" standard. Daniel, 891 F.3d at 767-768. Twombly and Iqbal's heightened pleading standards are inapplicable to determine Article III standing. Maya v. Centext Corp, 658 F.3d 1060, 1068 (9th Cir. 2011) (reversing a district court's order granting a 12(b)(6) motion for lack of Article III standing because the district court applied Twombly and Iqbal standards).

In Daniel, the expiration date of the plaintiff's debit card she used to buy a pass to a national park was printed on the receipt in violation of federal law. Subsequently, the plaintiff's debit card was used fraudulently, and she suffered damages from her identity being stolen. The plaintiff offered no facts to trace the printing of the expiration date on her receipt to the identity theft, did not claim that her receipt was lost or stolen or that a second copy of the receipt even existed. Rather, the plaintiff in Daniel merely asserted that a theft transpired at an unspecified time after the debit card transaction. Daniel, 891 F.3d at 767. Finding the link was not "fairly traceable", the plaintiff in Daniel had only asserted a broad allegation of harm subsequent to a statutory violation that was "divorced from" the violation. Id.

Here, Plaintiff's harm did not occur at an unspecified time after Twitter's misconduct. Rather, it started within a month after Alzabarah fled to Saudi Arabia, and approximately six months after Twitter allowed a KSA spy working for Twitter to access Plaintiff's account. (¶¶ 67, 69, 75, 122) What is more, Gamal Eid, executive director of a group that monitors human rights violations in the region stresses that the timing of the arrests of five other Saudi critics who had used anonymous Twitter accounts shows that the arrests are linked to the data stolen by the

two Twitter employees (¶ 95) Apart from Twitter letting KSA spies access Plaintiff's private user data and furnish it to KSA , nothing out of the ordinary had happened in 2014 or 2015 to have triggered this escalation of persecution beginning in December 2015. (¶ 121)

3. Twitter's Motion to Dismiss Distorts Plaintiff's TAC and Misapplies *Lujan*.

The following table illustrates Twitter's distortions of the TAC:

TWITTER'S FACTUAL ALLEGATIONS	THE TRUE RECORD
In 2009, Abdulaziz established himself as a well-known critic of KSA on Twitter. TAC ¶ 8 (Dkt. 99, 8:16-17)	Plaintiff was not well known as of 2009. TAC ¶ 8 makes no such allegation.
Abdulaziz did not suffer any direct harm from KSA for nearly three years after receiving the 2015 notice. (Dkt, 99, 11:14-17)	Nothing in the record supports the claim that Plaintiff actually received the 2015 notice Twitter claims it sent. Plaintiff's harm began less Than a month after Twitter tipped ff Alzabarah. Mr. Abdulaziz's emotional distress resulting from his family being persecuted by KSA is harm.
According to Plaintiff's prior complaints, KSA did not contact him until May 2018. (Dkt. 99, 11, fn. 6)	Prior complaints do not allege that no KSA contact occurred before May 2018.
KSA learned of Plaintiff's collaboration with Jamal Khashoggi through NSO's Pegasus software. (Dkt. 99, 12:16-18)	The TAC pleads no such thing.
Plaintiff concedes that public criticism of KSA and MBS made him a target for harassment and persecution, years before the spying. See TAC ⁋⁋ 9, 120, and FAC ⁋⁋ 9, 15-16, 18. (Dkt. 99, 15:23-16:1.)	None of these paragraphs in the FAC or TAC make any such concession. The claim ignores the difference between cancelling Plaintiff's financial assistance to targeting his family in Saudi Arabia for persecution and harassment to silence Plaintiff by way of torture by proxy.

Abdulaziz does not identify any particular Twitter information Alzabarah and Abouammo improperly accessed that would have led the KSA to target him, his friends, or his family." (Dkt. 99, 16:1-3).	This is assertion is incorrect as it ignores ¶¶ 88 and 89.
Abdulaziz's allegation that the KSA's persecution 'intensified' at some unspecified time is too vague. (Dkt. 99, 16:10-13)	The TAC provides a detailed timeline of when and how KSA's persecution intensified from 2015-2018. (¶¶ 94-95; 120-122, 130-141)
The KSA's 2018 Pegasus malware attack on Plaintiff's phone cannot be tied to access of Plaintiff's Twitter information three years earlier. Both events could be parts of a preexisting chain of persecution due to his being a prominent critic. (Dkt, 99, 16:17-20)	Pegasus did not become operational for KSA until Spring 2018. (¶¶ 123, 135) Twitter's assertion also ignores the steadily escalating persecution starting in 2015 (the same year as the Twitter breach) through 2018. (¶¶ 94-95; 120-122, 123-125, 130-141) It also ignores that the time it would have taken for KSA intelligence members to review and analyze the Twitter data from 6,000 users to decide who to prioritize as a target. (¶ 123)
"…in his lawsuit against NSO, Abdulaziz alleges that NSO sold the Pegasus System to the KSA in June 2017 and implies that it was operational at that time. See RJN Ex. A, ¶¶ 8, 48-53." "For instance, Abdulaziz states that '[NSO]'s representatives asked the Saudis to buy a new smartphone and provide them with its number in order to prove to them that Pegasus 3 was capable of infiltrating the	This distorts Plaintiff's lawsuit against NSO. Nothing in the cited paragraphs makes such an implication. A request by NSO to demonstrate a prototype does not mean KSA's version of Pegasus with its training and operational support requirements was ready in 2017. The NSO lawsuit does not say if KSA officials complied with this request,

phone by only knowing the mobile phone number.' RJN Ex. A, ¶ 49." (Dkt, 99, 16:23-25, fn. 8)"	purchased an operational system or even knew how to use the system in 2017.
"Abdulaziz still fails to explain what information in his Twitter account would have prompted the KSA to hack his phone using the Pegasus malware some three years later. Abdulaziz continues to (incorrectly) allege that the KSA viewed his direct messages, but he still fails to allege with specificity what information in these messages would have caused the KSA to increase its persecution. Compare TAC ¶ 125 with FAC ¶ 87." (Dkt, 99, 17:3-7)	This assertion ignores ¶¶ 88 and 89 and distorts ¶ 125. ¶ 125 explains that although Abouammo and Alzabarah invaded thousands of accounts, KSA chose only a select few for early attach with the Pegasus. The Pegasus attack came after KSA's other attempts at silencing Plaintiff starting in late 2015 failed and Pegasus became operational in Spring 2018. What is more, Twitter demands that the Court apply a motion for summary judgment standard on a 12(b)(6) motion before Plaintiff has had the opportunity to conduct discovery. At the pleading stage, it is sufficient that among the thousands of user accounts that Twitter allowed KSA to raid, it appears KSA only chose to target Plaintiff with a Pegasus attack after trying for years to silence him in other ways.
"Abdulaziz's assertion that the KSA targeted his phone for hacking in 2018 because of what they learned from his Twitter account in 2015 is a conclusion, not a factual allegation, that stretches 'on information and belief' beyond any reasonable limit of plausibility." (Dkt. 99, 17-7-10)	Among thousands of accounts Twitter let KSA raid, it appears that only Plaintiff was in the first rank of Pegasus victims, (along with Jeff Bezos and a former high-ranking Saudi intelligence official). In the previous two years KSA had tried to silence him in other ways. Twitter offers no explanation to

	exonerate itself from this.[8] Twitter also fails to explain that if it was Plaintiff's ***public*** criticisms of KSA (which started in 2009) that was causing KSA to intensify its persecution of Plaintiff at the end of 2015, why KSA's persecution would continue throughout 2018 even though Plaintiff was greatly restricting his social media presence from January to July of that year. What further undermines Twitter's timeline is that apart from the Twitter data breach, nothing out of the ordinary had happened in 2014 or 2015 to explain KSA's escalation against Plaintiff in late 2015.

Twitter misrelies on Lujan to argue that "harm to third parties—and not to Abdulaziz personally—do not satisfy the Article III 'injury-in-fact' requirement." (Dkt. 99, 16:3-5). In Lujan the plaintiff sued to protect certain species of animals but did not show how damages to those species would harm the plaintiff. Members of the plaintiff entity did not even have concrete plans to return to the potentially affected areas to view these endangered species they claimed defendant would harm. Lujan v. Defs of Wildlife, 504 U.S. 555, 564 (1992). Here, KSA, after receiving private Twitter user data because of Twitter's poor security, persecuted Plaintiff's family, friends and correspondents in Saudi Arabia to pressure him to stop his political

[8] If Twitter wishes to establish that some other party is responsible for Plaintiff's damages, Twitter has the burden of proof on this point. Plaintiff is not required to preemptively negate it. Kellogg v. Asbestos Corp., 41 Cal.App.4th 1397, 1409 (1996); Hughey v. Candoli, 159 Cal.App.2d 231, 240 (1958); for pleading purposes Plaintiff need only establish that the facts are sufficient for a jury to decide that Twitter's negligence, however minor, was more than theoretical or infinitesimal. Bockrath v. Aldrich Chem. Co., 21 Cal.4th 71, 79 (1999).

activities, sent agents to Canada to confront him, infected his phone with malware when the technology became available and after years of other methods of silencing him had failed. They even sent a team to murder him.[9] Lujan does not preclude Plaintiff from recovering for the emotional distress, stress and anxiety from these episodes. Twitter just needs better security.

4. Twitter's Alibi Is Unpersuasive and Pushes a Bizarre Timeline.

Twitter, at the pleading stage, contests the TAC with the following timeline: Plaintiff began criticizing KSA publicly in 2009 and applied for asylum in 2013 after KSA cut off his financial assistance. In December 2015 (two years later), despite no change in Plaintiff's behavior and nothing out of the ordinary happening apart from Twitter's data breach, KSA suddenly escalated its persecution of Plaintiff in an unprecedented manner.[10] KSA steadily escalated its campaign against Plaintiff culminating in a Pegasus attack and sending a hit team to murder him in 2018. According to Twitter, this was all because of Plaintiff's public criticisms of KSA (that had started nine years earlier) despite Plaintiff greatly restricting his social media presence during the critical period from January 2018 to July 2018. Twitter fails to explain how this is plausible and provides no reason why KSA did nothing more than cut off his financial aid before 2014. Twitter's timeline lacks temporal proximity and is not plausible.

B. Plaintiff's Claims Are Timely Since He Did Not Receive the Defective December 11, 2015 Notice and Did Not Discover the Facts Until October 20, 2018.

Unless the TAC alleges "every fact which the defendant would be required to prove if he were to plead … statute of limitation as an affirmative defense", the matter cannot be resolved on the pleadings. Lockley v. Law Office of Cantrell, Green Pekich, Cruz & McCort, 91 Cal.App.4th 875, 881 (2001); see also United W. Medical Ctrs v. Sup. Ct, 42 Cal.App.4th 500, 505 (1996).

---

[9] An injury need not be tangible. Even the risk of real harm can suffice. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016) (internal citations omitted).

[10] Twitter insists that the persecution Plaintiff suffered from 2015-2018 are common KSA tactics used to discourage dissident activity. (Dkt. 99, 11:22-23). Twitter fails to mention why KSA waited until 2015 to start using such methods against Plaintiff and why it is more plausible than not that the Twitter hack that same year and Twitter tipping off Alzabarah less than one month prior to the start of the 2015 persecution had nothing to do with it.

Twitter confuses informing Plaintiff and sending a notice that Plaintiff never received. Sending a notice does not mean it was received and read. There are no allegations in the TAC or judicially noticeable facts indicating that Mr. Abdulaziz received the 2015 notice. No authority holds that a defendant sending a notice that a plaintiff did not receive starts the statute of limitations clock. Plaintiff unequivocally states he "did not receive the weak and unhelpful December 11, 2015 notification in any way" and states on information and belief that Twitter did not send him the notice (¶¶ 113, 119) Plaintiff has never even hinted that he received this notice.

Even were this Court, at the pleading stage, to credit Twitter's claim that it sent Plaintiff the December 11, 2015 notice and go even further to find that he actually received it despite the TAC's allegations, its defects[11] still mean that the duty of inquiry would not have been triggered by the notice because it was false and misleading in the following ways:

DEFECT	**WHY THIS IS MATERIAL**
Did not say that it was a KSA[12] inside job.	Plaintiff would not have cared if it was a country he did not criticize (e.g. Micronesia). Since Plaintiff had two factor identification on his Twitter account, an outside job would not have been nearly as dangerous as the inside job that Twitter allowed which allowed for hostile alteration of his private account information.
Did not say what the victims had in common (critics of KSA).	This would have warned any reader that KSA had embarked on a campaign to steal dissident user data.
Watered down to dishonesty: claims the recipients "may have"	Given the FBI's notice and Alzabarah's admission, Twitter had no reason to doubt that the raid of private user

[11] Twitter argues that the Court did not find persuasive Plaintiff's prior arguments that the December 11, 2015 was defective, and that the TAC adds nothing to cause reconsideration. (Dkt. 99, 19:21-23). However, the prior order did not address the December 11, 2015 notice's defects.

[12] Twitter claims Plaintiff "must have" known it was KSA (Dkt. 99, fn. 9). The December 11, 2015 notice was a generic notice sent to multiple users and not Plaintiff. Expecting Plaintiff to deduce the identity of the unnamed state sponsor among nearly 200 countries is unreasonable.

been targeted and that Twitter had "no evidence they obtained your account information".	data had in fact happened. This provided a false sense of security, which was ambiguous at best, dishonest at worse and in either event misleading.
Twitter never updated the recipients of the notice.	Even if Twitter was ignorant of some things at the time, it does not excuse its subsequent failure to update users.
Claimed it had no further information it could provide at the time.	Twitter did have more information (see prior points above) given the FBI's notice and Alzabarah's confirmation. Twitter consciously decided to conceal information from its users. Twitter did have more information because the FBI gave it to them.

Twitter's close ties with KSA and the bad publicity (which would have hurt Twitter's bottom line) gave it every motive to not provide full disclosure. (¶ 113) Even Runa Sandvik, a security researcher who did receive the notice criticized it as "not terribly helpful". Those who did receive the notice were left more confused about what had happened. (¶ 103)

Twitter claims its "notifications were accurate and sufficiently detailed to warn its account holders without compromising the FBI's active, confidential criminal investigation" with Twitter was cooperating (Dkt 98, 18:27-28; 19:10-15). Not so. Twitter interfered with that FBI investigation by refusing to heed the FBI's request and tipping off Alzabarah (giving him both reason and opportunity to flee). Twitter also failed to notify affected users once the investigation was concluded that they were breached, and the state actor was Saudi Arabia. (¶¶ 97-99; 113)

The discovery rule is well established in California law. CACI 455. There are two alternate tests for triggering the limitations period: (a) a subjective one requiring plaintiff's actual suspicion that the injury was caused by the wrongdoing; (b) an objective one requiring a showing that a reasonable person would have suspected the injury was caused by the wrongdoing. The first to occur begins the limitations period. Nguyen v. Western Digital Corp (2014) 229 Cal.App.4th 1522, 1552. Properly pled, as it is here, belated discovery is a factual, rather than a

legal question. Id.; see also Romano v. Rockwell Internat., Inc. (1996) 14 Cal.4th 479, 487 ("resolution of the statute of limitations is normally a question of fact".)

Here, there was no way for Plaintiff to have known before October 2018 that Twitter employees stole his private data in an inside job and furnished it to KSA. It was not until October 20, 2018 that Plaintiff learned KSA had stolen his private Twitter data in an inside job. (¶ 119). Even the articles from the popular press that Twitter cited in its prior Motion to Dismiss undermine their claim. For example, the December 12, 2015 article by Ashley Carman, "Twitter users targeted by state-sponsored attackers", observes that "there isn't a direct tie between the accounts." None of the articles mention KSA. The December 13, 2015 article by Chris Johnston, "Twitter warns of government 'hacking'" mentions China and North Korea being "thought to be responsible for some cyber hacking of western companies and governments."[13]

C. Plaintiff Properly Pleads His Negligence-Based Claims.

1. Twitter's Negligent Supervision/Retention Arguments Lack Merit.

Twitter's argument that the TAC does not plead facts showing Twitter knew or should have known Alzabarah or Abouammo would become KSA agents fails for two reasons. First, it necessarily relies on an incorrect interpretation of the law. Plaintiff does not need to allege that Twitter knew or should have known before hiring them that the two would become KSA agents. It is enough for a negligent supervision/retention claim that Twitter should have known (even after they were hired) they posed a risk to others. CACI 426 (emphasis added). Second, Twitter misconstrues the TAC. In essence, Twitter's security infrastructure included a system that generated real-time warning alerts when invasions of private user data occurred. A system without those warning alerts falls short of industry standards and constitutes failure to supervise. Twitter's disregard of the warning alerts constituted at least negligent supervision/retention of the two employees that were invading private user data. See CACI 426

[13] Regardless, media coverage does not impute suspicion for statute of limitations purposes. Nelson v. Indevus Pharmaceuticals, Inc. (2006) 142 Cal.App.4th 1202, 1206. Twitter concedes this point by omitting mention of such articles in its current Motion to Dismiss.

The two cases that Twitter cites are inapplicable. In Juarez v. Boy Scouts of Am., Inc., 81 Cal.App.4th 377 (2000), the California Court of Appeal affirmed a grant of a motion for summary judgment as to a negligent hiring/supervising claim involving a lawsuit by a former boy scout against the Boy Scouts of America and other defendants for sexual abuse by a scoutmaster. This was after discovery, which has not yet been permitted in the present case.

Doe v. Capital Cities, 50 Cal.App.4th 1038 (1996) was decided more than 20 years before the "MeToo" movement and Harvey Weinstein indictment. The plaintiff, an aspiring actor, sued ABC Entertainment for negligent hiring/supervision/retention of a director who allegedly drugged, bound, and raped plaintiff after inviting him to a work-related meal. Doe held that the plaintiff's allegations that ABC knew or should have known that the director bought and used mind-altering illegal drugs and used his position at ABC to gain sexual favors were insufficient as they were different from surreptitiously drugging and raping a potential employee. Id. at 1054-1055. The Doe court explained: "the cornerstone of a negligent hiring theory is the risk that the employee will act in a certain way and the employee does act in that way." Id. at 1055.

In April 2014 Twitter assigned Abouammo to work with a public relations firm that was representing KSA and to help that firm by verifying the private information identifying the ownership of a Twitter account tied to a "Saudi Arabian news personality." (Criminal Complaint, ¶ 25) Just one month later al-Qahtani was directly communicating with Abouammo asking him to verify another sensitive Twitter account. (Criminal Complaint, ¶ 26) Twitter knew or should have known that involving Abouammo in regular contact with extremely rich and politically powerful foreign officials of an authoritarian regime (that had been surveilling dissidents on Twitter to silence them) created the risk that he would at least be compromised. In fact, he was compromised. Abouammo even sent a message to Al-Qahtani, MBS' right hand man, on Twitter's own direct messaging platform declaring "proactively and reactively, we will delete evil, my brother." Twitter, despite being able to view this direct message, did nothing because Twitter could not be bothered to monitor an employee they made a liaison with KSA.

Beginning in December 2014 for Abouammo and May 2015 for Alzabarah, their improper accessing of private user data was setting off alerts in Twitter's security system. If

Twitter was paying attention to those alerts, it would have investigated the two, which would have revealed that they were improperly accessing private user data for KSA. This would have been even more apparent for Alzabarah, who invaded some 6,000 sets of private account information, ostensibly for work purposes, while he stayed in Saudi Arabia during a month-long personal leave from Twitter. Twitter utterly failed to supervise the two KSA spies in its employ by failing to monitor the alerts and as a result, negligently retained them without curtailing their improper access to private user data. KSA, a large investor in Twitter, must have been thrilled.

2. Plaintiff Properly Pleads Negligence.

a. Foreseeability

Twitter actually foresaw that employees could be bribed, as evidenced by its gift policies. But Twitter never enforced those policies, encouraging the two spies to believe they could abuse their positions of trust and steal confidential information with impunity. (¶¶ 13, 14)

Alzabarah and Abouammo each posed potential risks for Saudi activists who relied on Twitter's claimed privacy protections for direct messages and anonymity in the more public Twittersphere. Abouammo's job required him to form relationships with wealthy and politically influential Saudis. Alzabarah's greater technical expertise meant he could harvest massive amounts of data swiftly and easily. Yet Twitter made no effort to monitor their activities and ignored or never even detected the private data they were stealing. (¶ 33)

b. The Standard of Reasonable Care

While KSA's agents worked at Twitter, there were established industry standards for service providers (including Twitter) that stored private user data. The standards required restricting access to private data to workers who legitimately needed it to do their job. They also required monitoring for unusual system activity from users with authorized access, and real-time alerts that would call immediate attention to such activities. (¶¶ 49, 50)

c. Failure to Exercise Reasonable Care and Causation

Twitter refused to follow FBI guidelines to report foreign travel and contact. (¶ 82) In December of 2014 a top MBS aide gave Abouammo a watch valued at over $25,000. Although Abouammo's job required him to meet with wealthy and powerful Saudis, Twitter

lacked the proper safeguards in place to monitor Abouammo's activities, rendering Twitter's policies to protect against this very danger meaningless and thereby posing a risk to users (the very risk Twitter's Playbook meant to address). (¶¶ 43 & 44)

Almost immediately after receiving an expensive watch, Abouammo began accessing private user data from the Twitter account operated by Saudi whistle blower, Mujtahid ibn Harith ibn Hamam ("Mujtahid"), including his direct messages. On information and belief Abouammo saw Mujtahid's direct messages with Plaintiff. Twitter's security let Abouammo do this seven times from December 2014 to February 2015 without being detected. (¶ 46)

Twitter short-changed and short-staffed its security software and operations, making it easy for the two spies to operate. (¶¶ 12, 29) Twitter also negligently, trained and supervised, its employees and allowed them unrestricted access to user data by employees whose jobs did not require it. Industry standards require an employee to apply for access to private user data and that grants of such applications are provided for a limited duration and scope. (¶¶ 28, 61)

Neither Alzabarah nor Abouammo had regularly accessed such private data before and had no reason to do so. Alzabarah did not start using Twitter's app to access this data until he began working for KSA. This should have been a red flag for Twitter. (¶¶ 52-53)

KSA recruited Alzabarah to access Plaintiff's private Twitter information (e.g. direct messages and other confidential data) and leak it to KSA. Beginning on May 21, 2015 Alzabarah used Twitter software called Profile Viewer to get users' recent IP information, logs of activity including direct messaging, browsers used, and biographical information. Alzabarah accessed Plaintiff's private information first on or about June 19, 2015, and again in July, 2015. Alzabarah took personal leave in July 2015 spending the entire month in Saudi Arabia. He traveled there with his Twitter-supplied computer which he used to raid private information of hundreds of other Twitter account holders. Twitter never curtailed this foreign-based activity, all occurring while Alzabarah was on personal leave. (¶¶ 60, 76)

On or about September 27 and 28, 2015, Alzabarah illegally accessed the private data of Mujtahid, who immediately complained to Twitter that his private data had been accessed.

Twitter was either unaware of these multiple intrusions or turned a blind eye to them until shortly before December 2, 2015, when the FBI told Twitter it knew of the data theft. (¶¶ 75-79)

Twitter failed to implement established industry security standards (e.g. restricting employee access to private user data and human monitoring for alerts that were sounding so Twitter could address them). Had it done so, it would have stopped Abouammo and Alzabarah from stealing Plaintiff's data and giving it to MBS' murderous regime. Twitter, a billion-dollar company, simply could not be bothered to spend adequately on essential security. (¶¶ 11, 29)

Twitter mistakenly claims that TAC ¶ 35 contradicts allegations that Twitter ignored alerts. Not so. TAC ¶ 35 bolsters Plaintiff's claim as it shows Twitter did not bother to investigate whether its employees were improperly accessing private user data. That Twitter may have been grossly negligent does not shield it from negligent supervision/retention claims.

Twitter insists that Plaintiff's allegation that Twitter ignored alerts is not plausible because the TAC alleges that Twitter belatedly notified some of the victimized users and suspended Alzabarah once it learned of his misconduct. This claim lacks merit. Twitter finally acting[14] when the FBI told it what its employee had done hardly exonerates Twitter's failure to prevent, detect, and interdict employees' improper access of private user data for nearly a year.

3. The TAC Sufficiently Pleads Proximate Causation at the Pleading Stage

i. Deciding Proximate Causation as a Matter of Law at the Pleading Stage Is Only Appropriate in an Extreme Case Where the Only Reasonable Conclusion is an Absence of Causation.

Generally, proximate cause is a question of fact not to be resolved at the pleading stage. Modisette v. Apple Inc., 30 Cal.App.5th 136, 152 (2018) Deciding proximate causation as a matter of law is only appropriate if "the ***only*** reasonable conclusion is an absence of causation." Id. (emphasis added). This is a high standard. Even a fifteen-year time gap has been held to create a factual question about causation, rather than a legal one. Balido v. Improved Machinery, Inc., 29 Cal.App.3d 633, 642 (1972); see also Duffy v. City of Oceanside, 179 Cal.App.3d 666

[14] As stated earlier, Twitter's response harmed the FBI's investigation by disregarding a simple request to not tell Alzabarah about the investigation.

(1986) (holding that even where there are "serious questions of causation" where a killing occurred four and a half years after a warning allegedly should have been given, the matter still could not be resolved as a matter of law). Proximate causation only becomes a legal question in extreme cases. See Weissich v. County of Marin, 224 Cal.App.3d 1069, 1084 (citing cases).

ii. Twitter Has Not Demonstrated That the Only Reasonable Conclusion in the Case at Bar is an Absence of Causation.

Despite Twitter's arguments to the contrary, Abdulaziz need not prove that Twitter's negligence was the sole cause of his harm. It suffices that Twitter's negligence is a substantial cause of injury, even if Twitter's negligence "operated in combination with other causes, whether tortious or nontortious." Uriell v. Regents of University of California, 234 Cal.App.4th 735, 746-747 (2015) "[W]here concurrent independent causes contribute to an injury" California courts apply the "substantial factor" test. State Dept. of State Hospitals v. Superior Court, 61 Cal.4th 339, 352 fn. 12 (2015). ***"Substantial" is a misnomer***. A plaintiff must merely show the factor is one "that a reasonable person would consider to have contributed to the harm." It must be more than remote or trivial and need not be the only cause. CACI 430. Even a very minor force is a substantial factor. Bockrath, 21 Cal.4th at 79; see also Rutherford v. Owens-Illinois, Inc., 16 Cal.4th 953, 985 (1997) (even 1.2 percent fault is substantial)

Causation can be concurrent. Where multiple factors cause harm, if a defendant's negligence is a substantial factor in causing plaintiff's harm, that defendant is responsible. A defendant "cannot avoid responsibility just because some other person, condition, or event was also a substantial factor in causing plaintiff's harm." CACI 431. The comparative fault doctrine is well-established. See Doupnik v. General Motors Corp., 225 Cal.App.3d 849 (1990) Further, "where a defendant's negligence is a concurring cause of an injury, the law regards it as a legal cause of the injury, *regardless of the extent to which it contributes to the injury*." Espinosa v. Little Company of Mary Hospital, 31 Cal.App.4th 1304, 1317-1318 (1995)

Here, the temporal proximity defeats Twitter's proximate cause argument. Twitter does not explain why KSA waited six years after Plaintiff began his public criticisms (rather than

approximately 6 months after it received his private Twitter data and less than a month after it tipped of Alzabarah) to begin targeting his family and friends to silence him.

Twitter's misrelies on Pipitone v. Williams, 244 Cal.App.4th 1437 (2016) to argue that Plaintiff's harm would have occurred even without Twitter's misconduct. Pipitone reviewed a motion for summary judgment rather than a demurrer. Id. The case arose from the murder of Ryann Bunnell, the daughter of the plaintiff, by her husband, Jesse Crow. The plaintiff sued two doctors for failing to report the suspected abuse of her daughter as required by the California Penal Code. The plaintiff alleged that the doctors knew or should have known that Bunnell's injuries were the result of her husband's abusive conduct and failed to report the issue to law enforcement. Id. at 1440, 1442. The appellate court conducted its own *de* novo review of evidence obtained in discovery and affirmed the grant of summary judgment. Pipitone concluded that there was no evidence the outcome would not have been different if the defendant doctors had reported the suspected abuse because (a) both the plaintiff and plaintiff's decedent had reported this and other abuse to the police, and that the decedent had added the warning that Crow "had guns and was involved with 'a lot of illegal things.'" Id. at 1460. Noting that no further action was taken even though the interviewing officer forwarded his report to two jurisdictions, arresting and incarcerating Crow would have required "a series of discretionary determinations" by police and courts which interrupt the chain of causation. Id. at 1461-1462.

The case at bar is analogous to Landeros v. Flood, 17 Cal.3d 399 (1976) where the California Supreme Court reversed the trial court's dismissal on a demurrer. Landeros addressed a doctor's failure to diagnose battered child syndrome after treating injuries from severe physical abuse on an 11-month-old infant by that infant's parents. After the medical team released the infant to the parents, the parents inflicted additional injuries on her that led to permanent damage. Id. at 405-407. The Landeros court reasoned that since battered child syndrome included the likelihood that the assault on the victim was "not an isolated, atypical event but part of an environmental mosaic of repeated beatings and abuse," the trial court erred in ruling as a matter of law that the defendant's negligence was not the proximate cause of plaintiff's injuries. The California Supreme Court also explained that the plaintiff should have been permitted to prove

by expert testimony that defendants should have reasonably foreseen that her parents were likely to resume their abuse if she were returned directly to their custody. Id. at 412.

Landeros demonstrates that the present case should not be decided as a matter of law without discovery. Specifically, Twitter cannot exonerate itself by pointing to KSA's wrongdoing any more than the doctor in Landeros could point to the parents' child abuse. Just as the defendant in Landeros had a duty, Twitter had a duty to have adequate security systems. Twitter's breach of that duty allowed harm to Plaintiff at the hands of KSA just as Landeros' breach allowed harm to an infant at the hands of her parents.. Twitter could have prevented or at least mitigated Plaintiff's harm if Twitter had proper security protocols. Mr. Abdulaziz should be permitted to conduct discovery and demonstrate, through expert testimony, the industry standard of security and that Twitter should have reasonably foresee that lackluster security systems would likely lead to theft of private user data and resulting harm to its users.

In Uccello v. Laudenslayer, 44 Cal.App.3d 504 (1975), a landlord knew a tenant had a vicious dog but let it stay on the premises where it injured the tenant's family's guest. There were "Beware of Dog" signs on the property. The dog had attacked others in the past. Per Cal. Civil Code §1714: "Everyone is responsible, not only for the result of his willful acts, but also for an injury occasioned to another by his want of ordinary care or skill in the management of his property or person…" Uccello relied on the California Supreme Court's holding that ***absent a statute declaring an exception to section 1714's fundamental principle, "no such exception should be made unless clearly supported by public policy."*** Id. at 510 [citing Rowland v. Christian, 69 Cal.2d 108, 112 (1968)] (emphasis added). Since the landlord in Uccello could have terminated the tenancy unless the dog was removed, the landlord had enough control of the premises to be liable to third persons injured by a known danger. Id. at 512-513.

California presumes liability unless public policy clearly supports an exception per six enumerated considerations: (1) foreseeability of the harm to the plaintiff; (2) degree of certainty that plaintiff suffered injury; (3) closeness of connection between defendant's conduct and the injury suffered; (4) moral blame attached to defendant's conduct; (5) policy of preventing future harm; (6) extent of the burden to the defendant and consequences to the

community of imposing a duty to exercise care with resulting liability for breach, and availability, cost and prevalence of insurance for the risk involved. Rowland, 69 Cal.2d at 113 Applying the Rowland factors, Uccello reversed entry of judgment of nonsuit. The danger of harm was foreseeable, the defendant could control the danger and the act was closely connected to the plaintiff's harm. As to morality, a defendant "cannot be permitted to knowingly stand aside" when he has power to prevent harm. Id. at 514.

Twitter has not and cannot identify a statutory exemption to section 1714 liability, leaving only the question of public policy. All Rowland principles favor holding Twitter liable: First, the harm to Plaintiff was foreseeable. ¶¶ 15-27. Second, given the allegations regarding Plaintiff's injuries, Twitter can hardly deny them. ¶¶ 122, 126, 135, 137-139, 141-142, 146, 162-163; 167-168. Third, as analyzed above, Twitter's failure to implement industry standard security safeguards (e.g. restricting employee access to private data and human monitoring of the alerts that sounded upon inappropriate access so it could address them) resulted in Plaintiff's private data being passed to KSA. 5-6 months after the breach and within a month after Twitter tipped off Alzabarah and ruined the FBI's investigation, KSA escalated its persecution of Plaintiff to an unprecedented level. The temporal proximity (5-6 months) shows that Twitter's misconduct and Plaintiff's injuries are closely connected.

Fourth, moral blame attaches to Twitter since it could have easily afforded the security to protect its users from a breach it should have seen coming. (See e.g. ¶¶ 11-12, 15-27; 73) Twitter warned Alzabarah immediately, destroying a federal investigation while dawdling over warning some of its own users (which did not include Plaintiff). Fifth, there are strong policy interests in preventing future harm as the result of Twitter's lackluster security system, especially given recent revelations that 1,000 employees and contractors could still read and even alter private account information. (¶ 51) Sixth, Twitter maintaining security to prevent breaches would not be burdensome given Twitter's wealth and importance of protecting data from despots. The established industry security standards support this. Accordingly, Twitter cannot escape section 1714 liability by statutory exception or public policy.

D. Twitter's TOS Does Not Bar Plaintiff's Negligence-Based Claims.

1. The TOS is Adhesive and Too Ambiguous to Enforce Against Plaintiff

California law defines a contract of adhesion as " . . . a standardized contract which, imposed and drafted by the of superior bargaining strength, relegates to the subscribing party only the opportunity to adhere to the contract or reject it." American Bankers Mortgage Corp. v. Federal Home Loan Mortgage Corp., 75 F.3d 1401, 1412 (9th Cir. 1996) Importantly, California law does not limit this analysis to contracts for goods or services where there are no reasonably available alternatives. Twitter's proffered TOS is a classic contract of adhesion and is therefore unconscionable by definition. Flores v. Transamerica Homefirst, Inc., 113 Cal. Rptr. 2d 376, 382 (2001), *accord*, Shroyer v. New Cingular Wireless Servs.,498 F.3d 976, 983 (9th Cir. 2007).

An adhesive contract is unenforceable if it is both procedurally and substantively unconscionable. Armendariz v. Foundation Health Psychare Services, Inc., 24 Cal.4th 83, 115 (2000) (overruled on other grounds in ATT Mobility LLC v Concepcion, 563 US. 633, 340 (2011). Substantive unconscionability occurs where a provision in a one-sided contract serves no purpose other than to give the drafter an unfair advantage. Soltani v. Western & Southern Life Ins. Co., 258 F.3d 1038, 1040 (9th Cir. 2001). A naked disclaimer of liability such as the one found in Twitter's TOS epitomizes an agreement that benefits only one of the contracting parties.

Any ambiguity in a contract of adhesion must be construed against the party drafting it. Daniel v. Ford Motor Co., 806 F.3d 1217, 1225 (9th Cir. 2015). A contract is ambiguous if it is susceptible to two different meanings. Curry v Moody, 40 Cal.App.4th 1547, 1552 (1995). "[A]t the motion to dismiss stage, ambiguities in contract terms must be resolved in favor of the non-moving party." Snider v. Wells Fargo Bank, N.A., 2019 U.S. Dist. LEXIS 62622, *15 (N.D. Cal. February 12, 2019). The rules of interpretation consider a contractual term in the context of other terms in the contract with an eye toward harmonizing them. McCaskey v. California State Automobile Ass'n., 189 Cal.App.4th 947, 970 (2010).

The limitation of liability clause reads in pertinent part: "[T]o the maximum extent permitted by applicable law, the Twitter Entities shall not be liable for [damages] resulting from: (i) Your access to or use of or inability to access or use the services; (ii) Any conduct or content

of any third party on the services, including, without limitation, any defamatory, offensive, or illegal conduct of other users or third parties" (RJN, Ex. B, "Limitation of Liability").[15]

And what are the "Services"? "Services" are Twitter's "various websites", even if unknown to the user. They are "SMS, APIs, email notifications, applications, buttons, widgets, ads, and commerce services." "SMS" and "API" are not defined at all. "Content" is described as "any information, text, graphics, text, photos or other materials uploaded or downloaded or appearing on the Services." Nothing warns that private information Twitter does not put on a website but stores on servers is unprotected. "Transmissions" is not defined anywhere.

The exculpatory provision in subsection (ii) is even more problematic. Twitter seeks to be held blameless for harm "that results from" a user's access to or use of services or Content. But the harm Plaintiff suffered did not result from that access. It resulted from Twitter's lackluster security that allowed the targeted theft of his private information by KSA agents in Twitter's employ empowered to use Twitter's software and Twitter' s disregard of alerts when information was stolen. Second, as with subsection (i) it is at the very least unclear whether the "services" include data stored on servers but not broadcast to the web. Third, this subsection's reference to "Content" does not refer to private user information. "Private user information does not appear on the Twitter website, It is unclear whether private user data is even included in the definition of "content". Fourth, Twitter's TOS strongly suggests that the private information will be kept private. Section 3 of the TOS instructs users to employ strong passwords. It then states: "Twitter cannot and will not be liable for any loss or damage arising from your failure to comply with the above." This suggests that Twitter treats loss of the password-protected private data as a special case, and that Twitter will not deny liability for the loss of private information so long as the user has reasonably strong password protection. This is, at the very least, an ambiguity of Twitter's own creation, and it is a universally accepted maxim that such ambiguities

---

[15] See also Viotti v. Giomi, 230 Cal.App.2d 730, 739 (1964) (A general disclaimer of liability will not immunize someone from their own negligent acts. And exculpatory clauses are to be "strictly construed against the party asserting the exemption, especially where he is the author.")

are to be construed against the drafter. Mastrobuonno v. Shearson Lehman Hutton 514 U.S. 52, 63, 115 S.Ct. 1212, 1218, 131 L.Ed. 2d 76, 88 (1995); Int'l Bhd. of Teamsters, Local 396 v. NASA Servs. 957 F.3d 1038, 1042 (2020).

Most importantly, "[t]he whole of a contract is to be taken together, so as to give effect to every part, if reasonably practicable, each clause helping to interpret the other. Cal. Civ. Code §1641. California case law consistently reaffirms the primacy of this principle . . ." Id.

Twitter's own Terms of Service document is a single, organic document, and Twitter cannot now amputate one limb of the TOS (the password section on page 3 of the TOS) from another (the limitation of liability section on p. 9 of the same document.) If Twitter had not wanted to discuss its liability for surrendering password-protected information as part and parcel of its TOS, it should have created a separate document, instead of inferring that if users have reasonably strong password protection, Twitter will not deny liability. However, that they are not different documents suggests that Twitter treats loss of the password-protected private data as a special case, and that Twitter will not deny liability for the loss of private information so long as the user has reasonably strong password protection.

Twitter's reliance on Food Safety Net Servs v. Eco Safe Sys, USA, Inc., is misplaced as it does not mention the public interest prong. 209 Cal.App.4th 1118, 1126 (2012) [citing Tunkl v. Regents of University of California, 60 Cal.2d 92, 98-100 (1963)]. Further, one of the hallmarks of adhesion contracts (unequal bargaining power) is absent in a contract between a national manufacturer of food disinfection equipment and a large commercial laboratory.

The California Supreme Court has long held that exculpatory clauses in negligence cases are void as against public policy where they affect the public interest. Tunkl v. Regents of University of California, 60 Cal. 2d 92, 96 (1963); Vandermark v. Ford Motor Co., 61 Cal.2d. 256, 262-263 (1964). In Tunkl the Court recognized that defining such matters would inevitably be debated, but identified public interest characteristics that would render exculpatory language in a contract of adhesion is unenforceable: (1) The party seeking exculpation is often a matter of practical necessity for at least some members of the public; (2) the party holds itself out as being willing to perform this service for any member of the public; and (3) the party seeking

exculpation is in a business that is suitable for public regulation; (4) The essential nature of the service gives the party demanding exculpation superior bargaining power, making no provision for the counterparty to pay a fee for protection against negligence; and (5) the resultant control of the seller leaves the consumer vulnerable to the seller's negligence. Id. at 98-101.

Nearly all of the Tunkl factors are present here. First, anyone who wanted to reach Saudis had to develop a viable Twitter presence. (¶¶ 152-153) Indeed, Twitter actively strove for this control over a market segment as the key to increasing ad revenue. For Saudi activists nothing really compares to Twitter. Saudi Arabia, with a smaller population than California,[16] has the fifth highest number of Twitter users in the world[17]. (¶¶ 17, 152) This is why McKinsey, when it wanted to study voices critical of KSA, analyzed Twitter activity. Since 2011, most Saudis were shifting from Facebook to Twitter because the latter was geared more towards news on the Arab Spring. Public figures also started to create Twitter accounts. For Saudis as of 2011, Twitter was a platform to spread political ideas while Facebook was to keep in touch with friends. Saudis viewed Facebook as more of a social platform, only interacting with their friends, whereas Twitter was seen as a political platform. If Plaintiff were to use Facebook, Saudis would not hear his voice. The impact of Facebook vs. Twitter in Saudi Arabia is also evidenced by Saudi officials and ministers having verified accounts on Twitter but largely ignoring Facebook (¶¶ 152-153). Also, where Facebook requires giving up one's real name and imposes a limit of 5,000 "Friends", Twitter allows aliases and provides for unlimited followers (Plaintiff has over half a million.) (¶¶ 154-155) Twitter provides other crucial features that Facebook lacks (e.g. anonymity, hashtags) (¶ 155) Instagram is also not comparable to Twitter for Plaintiff's purposes. (¶ 156) Finally, it was Twitter that was a key means of communication for protestors in the Arab Spring that threatened Saudi Arabia until KSA unveiled a populist

---

[16] A Google search reveals that as of 2018, California's population was approximately 39 million while Saudi Arabia's was less than 34 million.

[17] 5 Social Media Trends in the Middle East in 2019 https://ijnet.org/en/story/5-social-media-trends-middle-east-2019 last visited October 29, 2020.

$130 billion social spending package. From 2011-2013, Facebook's market share in Saudi Arabia was sharply declining while Twitter's growth was exponential. (¶ 153)

Second, there is no doubt that Twitter holds itself out as being willing to offer a platform to any member of the public (except maybe certain outgoing presidents who incite insurrections of the Capitol Building). Third, social media companies like Twitter are suitable for public regulation as evidenced by what happened to Plaintiff, but also by recent Congressional concern (e.g. recent discussions about ending or limiting the immunity provisions in the Communications Decency Act and the Justice Department's recently filed an antitrust complaint against Google.[18] In an even more extreme case, social media, left to self-regulate and focus on revenue rather than safety, has contributed to the Myanmar genocide of Rohingya Muslims). Facebook is currently fighting an effort to subpoena its documents for a trial of Myanmar's crimes before the International Court of Justice.[19] (¶ 157)

Fourth and fifth, Twitter had complete control of the "agreement", presented on a 'take it or leave it' basis. Protection against negligence was unavailable at any price as this was not part of the contract. This left Plaintiff utterly vulnerable to Twitter's negligence. Plaintiff's "choice" was to either forego the biggest audience for his criticize KSA or risk damages from Twitter's negligence. (¶ 150) This is ironic as this is a similar dilemma that individuals living inside Saudi Arabia must face: either shut up or be damaged.

In a subsequent decision elaborating upon Tunkl the California Supreme Court noted that California courts invalidated releases for even "*ordinary* negligence" where the release affected a public interest. City of Santa Barbara v. Superior Court, 41 Cal. 4th 747, 757 (2007) (emphasis in original). What is striking about these cases is the breadth of activities found to trigger the public interest analysis arising from essential services, including a Porsche dealership, Gardner

---

[18] https://www.nytimes.com/2020/10/22/technology/facebook-antitrust-f7tc.html, last visited October 27, 2020) and https://www.nytimes.com/2020/10/20/technology/google-antitrust.html last visited, October 27, 2020.

[19] In re Application Pursuant to 28 U.S.C. §1782 of the Republic of Gambia v. Facebook Inc., Case 1:20-mc-00036 (D., D.C.)

v. Downtown Porsche Audi, 180 Cal. App.3d 713 (1986), a residential landlord, Henrioulle v. Marin Ventures, Inc., 20 Cal.3d 512, 517-520 (1978); a childcare service provider, Gavin W. v YMCA of Metropolitan Los Angeles,106 Cal.App.4th 662 (2003), a yacht harbor, Pelletier v. Alameda Yacht Harbor, 188 Cal.App.3d 1551 (1986), a commercial bank, Vilner v. Crocker National Bank, 89 Cal.App.3d 732 (1979), and a title insurance company Akin v. Business Title Corp., 264 Cal.App.3d 153 (1968), Twitter, with its billions of users, cannot seriously argue that it is less of an essential service than a luxury car dealership or a yacht harbor.

Finally, Twitter is on a slippery slope when it compares the efforts to bring freedom and accountability to over thirty million people under the control of murderous despots – *with ski equipment* Olsen v. Breeze, Inc. 48 Cal.App.4th 608 (1996). And almost none of the conditions precedent upon which Olsen relied have any pertinence to this case. Olsen relied on three factors entirely absent here: (1) Skiers already assume the risks inherent in the sport; (2) the releases deal with risks associated with negligent acts that increase those inherent risks; (3) skiing is not an essential activity (much less a constitutionally protected one); (4) ski consumers were not denied a meaningful choice due to the common use of releases and (5) the release agreements are short. Id. at 621-622. In contrast, there are no risks inherent in using Twitter (like there are with falling from skiing) and therefore Twitter's exculpatory language does not increase an inherent risk. Further, as analyzed in depth below, Plaintiff had no reasonable alternatives apart from Twitter. Twitter's agreement is anything but short. It is ten pages long, uses undefined technical terms, and cross-references other documents. Finally, the false equivalence of skiing (a non-essential activity) with battling for free expression and democracy simply beggars the imagination. Recent events prove that the battle for democracy and accountability is absolutely essential. The people of Saudi Arabia should not be denied such freedoms because Twitter does not want to take responsibility.

Part of the ever-narrowing reach of exculpatory clauses has to do with judicial distrust of contracts of adhesion. Although exculpatory clauses may not generally affect public policy, "a contract entered into between two parties of unequal bargaining strength, expressed in the language of a standardized contract, written by the more powerful bargainer to meet its own

needs, and offered to the weaker party on a 'take it or leave it' basis carries some consequences that extend beyond orthodox implications. Akin, 264 Cal.App.2d at 158-159, quoting Gray v. Zurich Ins. Co., 65 Cal.2d 263, 269 (1966).

Accordingly, it would be inappropriate to conclude as a matter of law that Plaintiff agreed to be without protection from Twitter's lackluster security letting employees invade his private user data information and provide it to KSA to intensify its persecution of Plaintiff.

Relying on Darnaa LLC v Google LLC, 756 Fed. Appx 674 (9th Cir. 2018) and Lewis v. You Tube, LLC, 244 Cal.App.4th 118 (2015) Twitter argues that because it provides a "free" service, it should be absolved of liability. The argument fails for three reasons: First, neither Darnaa nor Lewis involved issues of whether the TOS contained ambiguities. Second, it was the plaintiff in Lewis who sought to enforce the TOS.

Third, the premises underpinning Lewis's language about free services are absent from this case (and are absent from Lewis, for that matter.) In reaching its "free services" exception Lewis relied on a single case, Markborough California, Inc. v. Superior Court 227 Cal.App.3d 705, 714 (1991), which stated "limitation of liability provisions are particularly important where the beneficiary of the clause is involved in a high-risk, low compensation service." Examining Markborough vividly illustrates why its principles say nothing about Twitter. Markborough concerned an engineer alleged to have failed to design a proper liner for an artificial lake. There was never a suggestion that the petitioner in Markborough received "low compensation", and Twitter, with its $2.2 billion in revenue in 2015 (⁋ 11) can hardly be said to be providing a 'low compensation' service. That Twitter does not charge its users does not mean it is not wildly profitable. It just monetizes its service in a way different way (e.g. advertising and licensing data) (see ¶ 151). The second Markborough prong of a "high risk" service may possibly apply to an artificial lake, but certainly does not apply to Twitter. . More centrally Markborough emphasized that the contractor's offer letter to Markborough "indicates that Markborough had an opportunity to request a change in any provision of the contract, including the limitation of liability clause." Id. at 716. This is precisely what Twitter denied Plaintiff (see ¶ 150). This is fatal for, as even Markborough observes, "a contract provision may be unconscionable if the is

an 'inequality of bargaining power which results in no real negotiation and an absence of meaningful choice." Id. at 715. Indeed, Markborough holds that "the common law sanctioned the use of limitation of liability clauses so long as they were not against public policy and not unconscionable". Id. Thus the very precedent that supposedly underpins Lewis is a compelling example of why it does not apply to the present case.[20]

Fourth, Darnaa was premised in part on the finding that because there were "reasonably available alternatives" to Google, there was no unconscionability. This was not true of Twitter in 2015 and was certainly not true of it when Plaintiff joined in 2011. At that time there was nothing like Twitter and activists throughout the Middle East (and indeed around the world) depended upon Twitter as their only same means to broadcast their messages to one another. The severe and near-total repression of public speech in in Saudi Arabia caused Plaintiff to exclaim, "Twitter is our Parliament." (¶ 19) Fortunately for Twitter's profits and unfortunately for its argument on this issue, there were no reasonably available alternatives to Twitter.

III. REQUEST FOR LEAVE TO AMEND

If the Court grants all or part of Twitter's motion to dismiss, Plaintiff respectfully request leave to amend to address any such issues. All of Defendant's arguments, if found to have merit, would become moot if Plaintiff were to have leave to amend to address them.

IV. CONCLUSION

Plaintiff's adequately pleads Article III standing and states a claim upon which relief may be granted. Accordingly, Twitter's motion to dismiss should be denied. If the Court grants all or part of Twitter's motion to dismiss, the Court should grant leave to amend.

DATED: January 13, 2021

RESPECTFULLY SUBMITTED

KLEIMAN / RAJARAM

By: /s/ Mark Allen Kleiman, Esq.
Mark Allen Kleiman, Esq.

LAW OFFICES OF BEN GHARAGOZLI
Ben Gharagozli, Esq.

[20] There are also public policy considerations to not immunize Twitter from liability. (See ¶ 157)